DETAILED ACTION

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Henry N. Blanco White (Registration Number 47,350) on 04/29/2010. According to the Attorney's telephonic discussion, Applicant agreed to amend Claims 32-34, 44-45, 52-53, 55 and cancel Claims 54 and 56.

The application has been amended as follows:

32. (Currently Amended) A transparent encryption appliance that does not store data for protecting data received from a web stored in a database by a web server environment, the transparent encryption appliance comprising:

at least one client interface for coupling to at least one network and communicating with one or more clients via the at least one network;

a server interface for coupling to ~~a~~ the web server environment;

wherein the appliance is separate from the web server environment and is operative to be connected between the web server environment and the at least one network, wherein the server interface and the at least one client interface communicate using ~~the~~ same communications protocol; and

a processor coupled to the at least one client interface and the server interface for at least one of securing and unsecuring data, wherein:

securing data comprises: evaluating a data transaction received through the at least one client interface; identifying first sensitive data contained in said data transaction; securing only the first sensitive data by at least one of encrypting, hashing, and keyed hashing; replacing in the data transaction the identified first sensitive data with the secured first sensitive data; and providing the data transaction including the secured first sensitive data through the web server interface; and

unsecuring data comprises: responsive to a request received through the at least one client interface for second sensitive data corresponding to at least a portion of the stored secured first sensitive data or other stored secured sensitive data, receiving through the web server interface the secured second sensitive data corresponding to the requested data; unsecuring the received secured second sensitive data by at least one of decrypting and hash verifying; and providing the unsecured second sensitive data through the at least one client interface.

33. (Currently amended) The appliance of claim 32, wherein:

in securing data the data transaction is received through a first said client interface; and

in unsecuring data the request is received, and the unsecured second sensitive data is provided, through[[,]] the first said client interface or a second said client interface.

34. (Currently amended) The appliance of claim 32, wherein the processor manages SSL traffic and handles computations that support SSL connections, wherein at least one of:

in securing data the data transaction is received via a first SSL connection and SSL computations are completed before identifying the first sensitive data contained in the data transaction; and in unsecuring data the unsecured second sensitive data is provided via a second SSL connection.

44. (Currently amended) A system for protecting data stored in a web server environment, comprising:

at least one client coupled to at least one network;

~~a~~ the web server environment that stores data received from ~~the~~ a web in at least one database and does not secure by encrypting, hashing, or keyed hashing the data received from the web before ~~it~~ the data is stored; and

a transparent encryption appliance separate from the web server environment and connected between the web server environment and said at least one network that does not store data for protecting the data stored in the web server environment, comprising:

at least one client interface coupled to the at least one network and communicating with the at least one client via the at least one network;

a server interface coupled to the web server environment, wherein the server interface and the at least one client interface communicate using ~~the~~ same communications protocol; and

a processor coupled to the at least one client interface and the server interface for at least one of securing and unsecuring data, wherein:

securing data comprises: inspecting a data transaction received through the at least one network interface; identifying first sensitive data contained in said data transaction; securing only the first sensitive data by at least one of encrypting, hashing, and keyed hashing; replacing in the data transaction the identified first sensitive data with the secured first sensitive data; and providing the data transaction including the secured first sensitive data to the web server environment, wherein the secured first sensitive data is stored in said at least one database by the web server environment; and

unsecuring data comprises: responsive to a request received through the at least one network interface for second sensitive data corresponding to at least a portion of the stored secured first sensitive data or other stored secured sensitive data, receiving from the web server environment the secured second sensitive data corresponding to the requested second sensitive data retrieved from said at least one database by the web server environment; unsecuring the received secured second sensitive data by at least one of decrypting and hash verifying; and providing the unsecured second sensitive data through the at least one client interface.

45. (Currently amended) The system of claim 44, wherein the processor of the appliance manages SSL traffic and handles computations that support SSL connections, wherein at least one of:

in securing data the data transaction is received via a first SSL connection and SSL computations are completed before identifying the first sensitive data contained in the data transaction; and

in unsecuring data the unsecured second sensitive data is provided via a second SSL connection.

52. (Currently amended) A system for protecting stored passwords, comprising:

one or more clients coupled to at least one network;

a web server environment that stores data received from ~~the~~ a web and does not secure by encrypting, hashing, or keyed hashing the data received from the web before ~~it~~ the data is stored; and a transparent encryption appliance separate from the web server environment and connected between the at least one network and the web server environment and operative to protect passwords contained in the data stored in the web server environment, comprising:

at least one client interface coupled to the at least one network and communicating with the one or more clients via the at least one network;

a server interface coupled to the web server environment, wherein the server interface and the at least one client interface communicate using ~~the~~ same communications protocol; and

a processor coupled to the at least one client interface and the server interface for securing passwords, wherein securing a password comprises identifying a password contained in a data transaction received through the at least one client interface; securing the password by at least one of encrypting, hashing, and keyed hashing, while not securing the transaction as a whole; replacing in the data transaction the identified password with the secured password; and providing the data transaction including the secured password to the web server environment;

wherein, responsive to a request received through the at least one client interface of the appliance for an action requiring authorization and containing a password, the appliance secures the password contained in the request, while not securing the request as a whole, and provides the request including the secured password to the web server environment; the web server environment obtains the secured password from the provided request, retrieves a secured password previously secured by the appliance and stored by the web server, compares the obtained secured password to the retrieved previously stored secured password, and authenticates the action requiring authorization in the case the obtained secured password matches the retrieved previously stored secured password.

53. (Currently Amended) A method of protecting data stored in a web server that does not secure data by encrypting, hashing, or keyed hashing, comprising:

receiving from a client coupled to a network by a transparent encryption appliance that does not store data a data transaction containing first sensitive data, the transparent encryption appliance being separate from the web server and connected between the network ~~client~~ and the web server, wherein the transparent encryption appliance comprises at least one client interface coupled to the at least one network and communicating with the at least one client via the at least one network, and a server interface coupled to the web server, wherein the server interface and the at least one client interface communicate using same communications protocol;

~~identifying the sensitive data;~~

securing only the ~~identified~~ first sensitive data by: inspecting the data transaction; identifying the first sensitive data contained in said data transaction; securing only the identified first sensitive data using a processor coupled to the at least one client interface and the server interface by at least one of encrypting, hashing, and keyed hashing; replacing in the data transaction the identified first sensitive data with the respective secured first sensitive data; and providing the data transaction including ~~with~~ the secured first sensitive data to the web server; and

storing the provided secured sensitive data in a database by the web server, wherein the web server does not secure by encrypting, hashing, or keyed hashing the data received from the web before the data is stored; and

unsecuring secured sensitive data by: responsive to a request for second sensitive data corresponding to at least a portion of the stored secured first sensitive data or other stored secured sensitive data, retrieving from the database by the web server the secured sensitive data corresponding to the requested second sensitive data; forwarding the retrieved secured sensitive data to the transparent encryption appliance; unsecuring the received secured data using the processor by at least one of decrypting and hash verifying; and providing the unsecured second sensitive data to fulfill the request.

54. (Canceled).

55. (Currently Amended) A non-transitory computer readable storage medium storing executable instructions which, when executed in a computer, protect sensitive information stored in a web server by a method comprising:

receiving from a client coupled to a network by a transparent encryption appliance that does not store data a data transaction containing first sensitive data, wherein the transparent encryption appliance comprises at least one client interface coupled to the at least one network and communicating with the at least one client via the at least one network, and a server interface coupled to the web server, wherein the server interface and the at least one client interface communicate using same communications protocol;

inspecting the data transaction;

identifying the first sensitive data contained in said data transaction;

securing only the identified first sensitive data by at least one of encrypting, hashing, and keyed hashing using a processor of the computer;

replacing in the data transaction the identified first sensitive data with the respective secured first sensitive data;

providing the data transaction including ~~with~~ the secured first sensitive data to a web server that is separate from the transparent encryption appliance and that does not secure the data received by encrypting, hashing, or keyed hashing before the data is stored;

storing the provided secured sensitive data in a database by the web server;

responsive to a request for second sensitive data corresponding to at least a portion of the stored secured first sensitive data or other stored secured sensitive data, receiving at the transparent encryption appliance from the web server the stored secured second sensitive data corresponding to the requested second sensitive data;

unsecuring the retrieved second sensitive data by at least one of decrypting and hash verifying using the processor of the computer; and providing the unsecured <u>second</u> sensitive data to fulfill the request.

56. (Canceled).

Allowable Subject Matter

2. Claims 32-42, 44-50, 52-53, and 55 are allowed.

The following is an examiner's statement of reasons for allowance: Any prior art of the record does not teach or suggest alone or in combination with other prior art of record the specific features required in the independent Claims 32, 44, 52, 53, and 55 as "at least one client interface for coupling to at least one network and communicating with one or more clients via the at least one network; a server interface for coupling to a web server environment; wherein the appliance is separate from the web server environment and is operative to be connected between the web server environment and the at least one network, wherein the server interface and the at least one client interface communicate using the same communications protocol; and a processor coupled to the at least one client interface and the server interface for at least one of securing and unsecuring data, wherein: securing data comprises: evaluating a data transaction received through the at least one client interface; identifying first sensitive data contained in said data transaction; securing only the first sensitive data by at least one of encrypting, hashing, and keyed hashing; replacing in the data transaction the identified first sensitive data with the secured first sensitive data; and providing the data transaction including the secured first sensitive data through the web server interface; and unsecuring data comprises: responsive to a request received through the at least one client interface for second sensitive data corresponding to at least a portion of the stored secured first sensitive data or other stored secured sensitive data, receiving through the web server interface the secured second sensitive data corresponding to the requested data; unsecuring the received secured second sensitive data by at least one of decrypting and hash verifying; and providing the unsecured second sensitive data through the at least one client interface" recited in the independent Claim 32. The prior art taken either single or in combination fails to anticipate or fairly suggest the above limitations of applicant's independent claims in such a manner that a rejection under 35 U.S.C. 102 or 103 would be proper. Therefore, the claimed invention is considered to be in condition for allowance as being novel and non-obvious over prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Contact Information

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Baotran N. To whose telephone number is 571-272-8156. The examiner can normally be reached on Monday-Friday from 8:00 to 4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/B. N. T./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435